Marine Expeditionary Forces, with integrated aircraft and combat service support, along with Navy SEAL teams, submarines and battle groups are often the first to arrive in theater and must rely on spectrum to remain highly maneuverable, flexible and tactically effective.

the spectrum-dependent capabilities of the Navy and Marine Corps are preserved. Because the radio frequency spectrum must be shared among nations, a United Nations agency, the International Telecommunication Union, convenes the World Radiocommunication Conference to modify spectrum allocation as technology and services require.

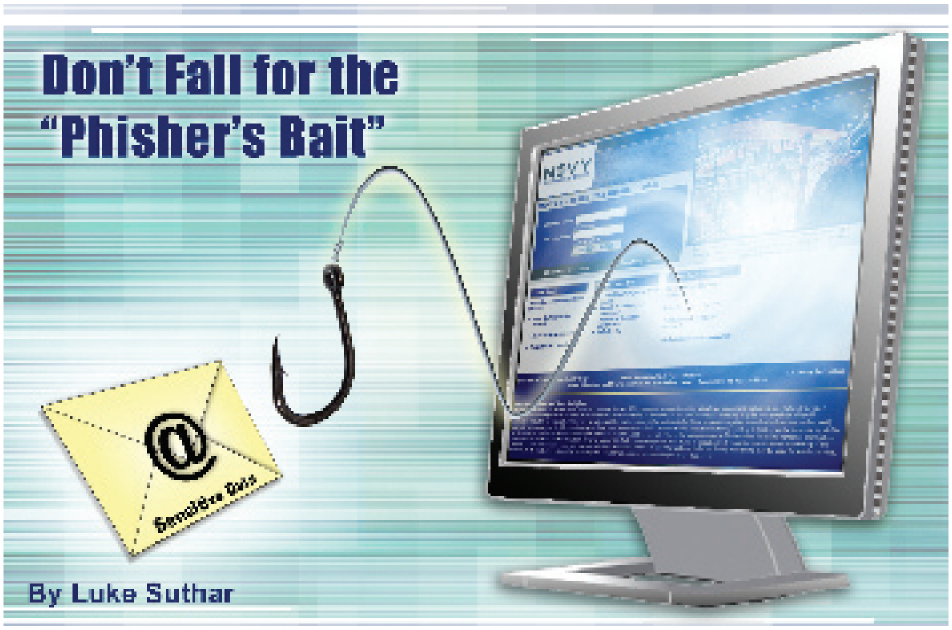
All members of the United Nations are invited to these conferences and the Department of the Navy Chief Information Officer participates as the Department's national and international representative to these forums.

To achieve its goals, the DON strives to improve efficient use of spectrum through collaborative efforts among business, industry, government and other nations.

In order to maintain America's advantage and secure our country's future, we must continue to work to meet our growing national spectrum challenges because electromagnetic spectrum is critical to both our nation's security and economy.

For more information, please contact the DON Spectrum Team at DONSpectrumTeam@navy.mil. CHIPS

Can You Hear Me Now is a regularly featured column in CHIPS magazine. Please go to the CHIPS Web site at http://www.chips.navy.mil/ and click on the Archives link at the top of the page to view past columns.



Don't Fall for the "Phisher's Bait"

By Luke Suthar

Department of the Navy (DON) networks are under continuous attack by an invasion of "spam on steroids." There has been a significant and widespread trend of using bogus e-mails to steal personal information and access critical DON information systems.

The ultimate objective of these Internet intruders is to trick unsuspecting users to open an attachment or click a Web link that will download specialized malicious software onto the computer. This process circumvents existing security measures and allows access to DON data.

The Naval Criminal Investigative Service (NCIS) has observed a growing trend of thousands of malicious e-mails targeting Sailors, Marines, Navy civilian workers and DON contractors, with the potential to compromise a significant number of computers across the Department.

Web Tricks

"Phishing" is a criminal activity in which an adversary attempts to fraudulently acquire sensitive information by impersonating a trustworthy person or organization using, for example, manipulated e-mails that appear to represent the DON, Navy Federal Credit Union, Navy Knowledge Online (NKO) or other familiar institutions.

The ultimate goal of a phishing attempt is to extract information through the contact in order to evade existing security measures and allow access to DON secure information and data. Phishing is typically carried out using two techniques: "spoofing" and "social engineering."

Spoofing an e-mail creates a fraudulent message with an e-mail address and page content that appear to be from a valid source. Often the e-mails contain malicious attachments and links to deceptive Web sites that appear to be an exact duplicate of the authentic Web sites.

Social engineering involves multiple correspondences to potential victims in order to get them to divulge critical and confidential information through trickery. Correspondence includes, but is not limited to, the use of e-mails, telephone calls and personal contact.

Victims are manipulated or tricked into providing personally identifiable information, such as credit card numbers, bank information, Social Security numbers, user IDs and passwords — and possible critical information that could harm the DON network that would not be otherwise easily disclosed.

When spoofing and social engineering are concatenated, the outcome is a new technique, known as "spear phishing" — a mass of manipulative e-mails to unsuspecting recipients who believe the message is authentic and from a trusted sender.

When using spear phishing, offenders adapt to security measures that would otherwise block a majority of these menacing e-mails. This type of attack uses targeted e-mails that are manipulated to specifically fit the potential victims, providing them with a false sense of trust.

Spear phishing is similar to phishing; however, the audience is a targeted group of individuals. The sophistication of this technique is reflected in the attacker's ability to obtain legitimate DON documents, use enticing subject lines relating to genuine operations, exercises or military topics, and exploit the trust of users across the Department.

The following are the steps attackers use to complete a spear-phishing scheme:

(1) The attacker obtains e-mail addresses for the intended victims and generates an e-mail that appears genuine and which requests the recipients to perform a certain task or action.

(2) The attacker sends the e-mail to the intended victims in a way that appears legitimate and obscures the true source.

(3) Depending on the content of the e-mail, the recipients open a malicious attachment, complete a form or visit a deceptive Web site.

(4) The attacker collects the victim's sensitive information for future exploitation.

Tips for Prevention

Be aware that providing personal information to an unverified source may lead to information compromise, identity theft and a great deal of stress. By taking the following few simple precautions you can help avoid this costly mistake:

Digital Signatures – The DON CIO issued naval message 061525Z of October 2004, Public Key Infrastructure (PKI) Implementation Guidance, which required DON network users to digitally sign any e-mail requiring message integrity and non-repudiation. Any message that tasks or requests a DON user to provide personal or otherwise sensitive information should be digitally signed. (Go to http://www.doncio.navy.mil and type 061525Z in the Search block to download a copy of the guidance.)

If a digital signature is not present and the sender is unknown, recipients should verify the authenticity through other methods, such as a phone call to verify and request a digital signature.

If the sender's identity still cannot be verified, the message should not be opened and the incident should be reported to the user's information assurance (IA) manager and/or the NMCI help desk immediately by phoning 1-866-THE-NMCI (1-866-843-6624).

User Education – Users should not answer any e-mail that attempts to collect personal identifiers and other critical information unless the e-mail has been verified to be authentic.

Opening e-mail attachments or clicking on hyperlinks from unknown or unexpected sources, including but not limited to e-mail from dot-mil and dot-gov sources, could cause a system malfunction, slow computer performance and ultimately disrupt network service.

Mandatory Training – To combat the growing threat of spear-phishing, the Navy Cyber Defense Operations Command issued Task Order 06-17 (INFOCON 4), which makes "DoD Spear-Phishing Awareness" training mandatory for all military, civilian and contractor employees of the Defense Department.

This training is available on the Joint Task Force Global Network Operations (JTF-GNO) Web site at: https://www.jtf-gno.mil/. You will need to use your Common Access Card to log in.

Some commands are offering in house training. Employees should check with their command IA manager or security manager for guidance.

Information assurance training offered on NKO provides additional details and preventive tips. To access the IA training, go to http://www.nko.navy.mil. If you are not a registered user, you must register first, then select the following options:

- Launch Navy E-Learning
- Browse Categories
- U.S. Department of the Navy (DON)
- Information Assurance (IA)
- Select DoD Information Assurance Awareness

User Reporting – NMCI users are encouraged to perform one of the two following directions upon receipt of spam or unwanted e-mail:

1. Highlight the spam e-mail in your Inbox, but do no open it.

2. Go to Edit > Copy.

3. Paste the entire e-mail into a new message, and ensure the word SPAM is in the subject line.

4. Forward it to GNOC_GL-IAM. The message will be forwarded to spam filter managers for action.

Laukik "Luke" Suthar is an NCIS special agent supporting the DON CIO.

CHIPS

The Joint Task Force Global Network Operations (JTF-GNO) offers DoD Spear-Phishing Awareness training at: https://www.jtfgno.mil/.

You will need to use your Common Access Card to log in.

Tips from the JTF GNO presentation of the DoD Spear-Phishing Awareness Training

Discovered "spear-phishing" messages within the DoD can be very convincing.

How to recognize a spear-phishing attempt

-"From" field of an e-mail can be easily faked (spoofed). It might appear completely correct, or have a similar variation. For example: account_security@mypay.com

-On the other hand, the message may come from a legitimate e-mail account, because that account has been compromised. For example: john.smith.yourboss@yourbase.mil. This can occur when the attackers obtain someone's login credentials and e-mail contacts.

How can I be sure?
Is the message digitally signed?

Other recognition factors of phishing attempts:
1) Generic Greeting
2) Fake Sender's Address
3) False Sense of Urgency
4) Fake Web Links. Deceptive Web Links.
E-mail requires that you follow a link to sign up for a great deal, or to log in and verify your account status, or encourages you to view/read an attachment.
5) E-mails that appear like a Web site
6) Misspellings and Bad Grammar

Be cognizant of this threat. Before clicking on any Web link within a message or opening up an attachment, be sure the source of the e-mail is legitimate! The importance of digitally signing your messages can't be stressed enough.